Troubleshoot Common Protected Roaming Client Errors

Contents

Introduction

This document describes how to troubleshoot common issues where a roaming client is protected but not behaving as expected.

Overview

Welcome to the "my roaming client" series of knowledge base article. This series provides an interactive series of questions in response to common roaming client challenges.

This document is targeted at the scenario where the roaming client is green and protected, but not behaving as expected. This document provides frequently asked questions for this scenario frequently seen after deploying roaming clients. The client installs, but is not behaving as expected.

The "My Roaming Client Series" Index:

1. My roaming client does not activate and....
2. My roaming client says "Protected" but....

Common Issues

Explore the possibilities in each subsection, by filling in the blank of "My roaming client says "Protected" but... __________":

Unknown, Unprotected

If this is the current state, this article is not targeted for this scenario! This represents an unprotected state where the client has not yet registered. See this article on ways a proxy can prevent a roaming client from registering or contact our support team for assistance.

No Sites are Blocked

The roaming client reports "Protected" when we are able to reach 208.67.220.220 and 208.67.222.222 for DNS over UDP 53 or 443 or if the client is set to disable due to a known policy. If the client reports a Protected mode, but blocks are not occurring, follow these steps:

1. Check for a proxy. In the case of a transparent or explicit proxy, the DNS resolved on the computer is re-requested and overridden by the proxy server. Using Umbrella with a proxy?
2. A third party software DNS proxy is overriding the roaming client's DNS responses
3. A different than expected policy is applying. See how to confirm the expected policy is applying here.

Incorrect Policy is Applying

The roaming client reports "Protected and Encrypted" or "Protected and Transparent", but roaming client policies are not applying:

1. Validate that the roaming client-based policy is the winning policy. If on network, and the network is higher in the policy order than the roaming clients, its policy applies. See this article on determining which policy is being applied or visit policy-debug.opendns.com for details.
2. Check for a proxy. In the case of a transparent or explicit proxy, the DNS resolved on the computer is re-requested and overridden by the proxy server. The proxy server using Umbrella would apply only its egress-based network level coverage. Using Umbrella with a proxy?
3. Using the AnyConnect Roaming Security Module? The standalone roaming client must not also be installed at the same time! If both ERCService.exe and acumbrellaagent.exe are running concurrently, this indicates both are installed. Uninstall the standalone Umbrella roaming client, and ensure no software management tools are reinstalling it.

Public or All DNS is Failing

In this scenario, all DNS fails to receive a response. A nslookup in the command prompt or terminal times our or fails, and browsers report DNS issues and fail to load pages:

1. A third party software DNS proxy is overriding the roaming client's DNS responses. Many softwares only override "website destination" A-records, allowing TXT records to pass freely. Since the roaming client checks for DNS availbility with TXT records, the roaming client activates even if all A-records do not reach Umbrella. Encrypted Umbrella DNS combined with the background software often leads to a failure to send DNS A-records.
2. A firewall has DNS protection built in or a "web protection" service, which can interfere with Umbrella.
3. If this occurs intermittently, this can be PAT/NAT exhaustion. The addition of the roaming client has increased the number of direct UDP connections out of the workstations' egress network. This intermittently causes either just DNS or all web traffic to fail. For more information, see this article on this port exhaustion and how changing the UDP timeout or validating your UDP connection limit can help.
4. Using the AnyConnect Roaming Security Module? The standalone roaming client must not also be installed at the same time! If both ERCService.exe and acumbrellaagent.exe are running concurrently, this indicates both are installed. Uninstall the standalone Umbrella roaming client, and ensure no software management tools are reinstalling it.

Local DNS Fails

In this scenario, any public record fails; however, domains on your internal domains list fail to resolve. If the local DNS servers are queried directly, the query succeeds.

1. Is the domain failing added to your internal domains list? Note, any search suffix is automatically dynamically added to the local (not cloud side) list. Any local-only domain not on this list fails to resolve correctly. Any local domain not on the list appears in your Dashboard reporting. Any domain on the list does not. Learn how local DNS works here.
2. Are the local DNS servers correct? Validate that the values stored inside the roaming client match your expectations. Validate that each server listed (see location in this document) is able to return the response. Let us pick one to send each local DNS request to. These match your DHCP lease or static assignment. If not, let us know by opening up a support case.
   - Mac: /var/lib/data/opendns/resolv_orig.conf
   - PC: C:\ProgramData\OpenDNS\ERC\Resolver#-Name-of-NetworkAdaptor.conf
3. Software or VPN compatibility. Does the issue only occur when on a VPN? If so, ensure that the VPN does not restrict where DNS can flow or that your VPN is not on our unsupported list. See our VPN compatibility article for more details.

The Client Shows Offline on the Dashboard

The roaming client sync process is instrumental to the client states as shown on the dashboard. The roaming client only activates when:

- At least one sync to our sync server (currently sync.hydra.opendns.com) has completed since client start
- One of the Umbrella DNS servers are available on port 443 or 53 UDP.

The dashboard state of the client is updated every sync (currently takes up to 60 minutes). Here are some possible reasons why these states are not be up to date:

1. The client's state has changed since the last sync. Note, the initial sync on boot is while the client is "offline" or not protected due to the requirement of sync to be protected.
2. The client experiences intermittent failure to sync due to network restrictions. An initial sync can have occurred, but subsequent sync updates fail, resulting in the client appearing offline.
3. The computer has switched networks since the last start of the client. For example, the computer was turned on in a bakery-cafe with sync access, then brought into the corporate network without sync access. The client remains Protected/Encrypted if DNS is available, but the Dashboard reports the client is offline.

The Computer Reports a "No Connectivity" Warning

When using the roaming client, computers on certain network environments can display a network connectivity "yellow triangle" indicator, but network access is fully operational. This can impact Microsoft applications such as Outlook, since they do not sync if the indicator is tripped.

1. This issue is a known design limitation in Windows. To resolve it permanently:
   - Windows 7/8: follow the hosts file instructions on this document.
   - Windows 10: Update to version 1709 or later and follow these instructions to modify either your Group Policy or registry to implement Microsoft's fix.

The Local DNS Entry for the Computer Disappears

The roaming client transparently forwards any DNS query to any domain in your internal domains list. When using the roaming client, you most often see two updates rather than one because we are changing the DNS on the machine. In the event that the record disappears:

1. Read this article to deploy a Microsoft hotfix for Windows 7 to prevent the record being deleted the moment the client enters the protected mode.